REMARKS

STATUS OF THE CLAIMS

Claims 6, 8, 11-13 and 21-23 are pending in the application.

Claims 6, 8, 11-13 and 21-23 are rejected.

Claim 6, 8 and 11 are amended, and, thus, claims 6, 8, 11-13, and 21-23 remain pending for reconsideration, which is respectfully requested.

No new matter has been added in this Amendment. The foregoing rejections are hereby traversed.

CLAIM REJECTION – 35 U.S.C. §102

Claims 6, 8, 11-13, and 21-23 are rejected under 35 USC 102(e) as being anticipated by Barlow et al. (U.S. Patent No. 6,038,551). Barlow is newly cited, and, thus, newly relied upon.

The independent claims are 6, 8, and 11, which are anticipatorily rejected by Barlow.

The independent claims 6, 8 and 11, using claim 6 as an example, are amended as follows:

> 6. (CURRENTLY AMENDED) A process of user authentication in a client computing apparatus, comprising:
>
> executing, in the client computing apparatus, a web browser that processes a protected web page to be received from network;
>
> storing on an integrated circuit card a certificate to access the protected web page received in the client computing apparatus and characteristic identifying information of a user ~~associated with the received protected web page~~;
>
> issuing by the web browser a certificate request to the user, in response to the receipt of the protected web page by the web browser of the client computing apparatus;
>
> reading by an integrated circuit card reader the integrated circuit card, in response to the issuing of the certificate request by the web browser ~~receipt of the protected web page by the web browser of the client computing apparatus~~;
>
> comparing identifying information input by the user with the characteristic identifying information of the user stored in the integrated circuit card; and
>
> in response to the comparing, providing the certificate stored on the integrated circuit card to the web browser of the

client computing apparatus to access the received protected web page.

Support for the claim amendments can be found, for example, in page 14, line 7 to page 15, line 23, of the present Application.

The Office Action primarily relies on Barlow's certificate exchange for performing an electronic purchase transaction between a user or purchaser and a merchant using Barlow's IC card (column 16, lines 6-15).

Barlow discusses a portable, multi-purpose, integrated circuit (IC) card and complimentary computer software which enables access and management of resources maintained on the IC card (Abstract). Therefore, Barlow discusses the API layer 36 used with the IC card 14 to manage resources maintained on the IC card (Abstract, column 9, lines 38-65). One of the administrative tasks performed by the IC card is management of certificates on the IC card (column 9, lines 38-65). One of the cryptographic functions performed by the IC card is adding, retrieving or deleting a certificate on the IC card (column 10, lines 1-19).

Barlow discusses, "When the application 34 requests a cryptographic function, the cryptographic services module 40 communicates with the IC card 14 and woks cooperatively with the IC card 14 to perform the cryptographic function without exposing the cryptographic resources maintained on the IC card 14 (column 10, lines 1-7). So the Office Action relies on Barlow's certificate exchange operation discussed in column 16, lines 6-37 and FIG. 7, steps 150-162. However, Barlow uses the certificate stored on the IC card differently than the claimed present invention, because in step 156 of FIG. 7, the certificate is retrieved from the IC card and in step 158 the certificate is transmitted to the merchant. In step 160, the merchant's certificate is received and passed to the IC card and in step 162 the merchant's certificate is verified at the IC card. More particularly, in Barlow, the IC card 14 and the commerce application 34 could exchange certificates to mutually authenticate each other (column 16, lines 11-14) and the IC card and the merchant exchange certificates for authentication (column 16, lines 15-37).

However, in contrast to Barlow, the claimed present invention, using claim 6 as an example, provides:

> executing, in the client computing apparatus, a web browser that processes ***a protected web page to be received from network***;
>
> ...
>
> ***issuing by the web browser a certificate request to the user***, in response ***to the receipt of the protected web page*** by the web browser of the client computing apparatus;
>
> ...; and
>
> in response to the comparing, ***providing the certificate stored on the integrated circuit card to the web browser*** of the client computing apparatus ***to access the received protected web page***.

In other words, in contrast to Barlow, the claimed present invention's Web browser issues a certificate request to a user when a protected web page is to be accessed, and the certificate stored on the IC card is used by a Web browser to access, for example, read, a secured or protected Web page(s) of a WWW server.

DEPENDENT CLAIMS 12 AND 21

Further, in contrast to Barlow, the claimed present invention as recited in dependent claims 12 and 21, using claim 12 as an example, provides:

> 12. (PREVIOUSLY PRESENTED) The computer system of claim 11, wherein the computer further comprises a display unit and the integrated circuit card program further performs:
>
> displaying on the display unit ***selectable names of protected applications as protected web pages***, if a result of the comparing of the user identifying information is matching; and
>
> the providing of the stored certificate comprises ***providing one of a plurality of certificates stored on the integrated circuit card and corresponding to a selected one of the protected applications by the user to the web browser to access the selected protected application***.

The Office Action relies on Barlow's column 13, line 20 to column 14, lines 20. Barlow, in FIG. 5, describes a user interface to manage resources maintained on the card. Barlow in column 13, lines 56-65, discusses, "For example, a certificate screen 114 permits the user to manage various certificates which have been issued for the public keys stored on the IC card and associated with various applications such as authentication, electronic payment, electronic

travel, etc." However, Barlow fails to disclose or suggest the claimed present invention's, "***providing one of a plurality of*** certificates stored on the integrated circuit card ... ***corresponding to a selected one of the protected applications by the user to the web browser to access the selected protected application***," because Barlow does not contemplate providing a certificate to a web browser to access a protected web page to be received by the web browser.

In view of the claims amendments and remarks, withdrawal of the rejection of pending claims and allowance of pending claims is respectfully requested.

CONCLUSION

If there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

Respectfully submitted,
STAAS & HALSEY LLP

Date: September 6, 2005

By: _____
Mehdi D. Sheikerz
Registration No. 41,307

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501